Title: SYSTEM AND METHOD FOR AUTHENTICATING THE DOMAIN OF A SENDER OF A MESSAGE
Invent rs: Mark Delany
Docket N : D&D No. 08226/100S142-US1

1/7
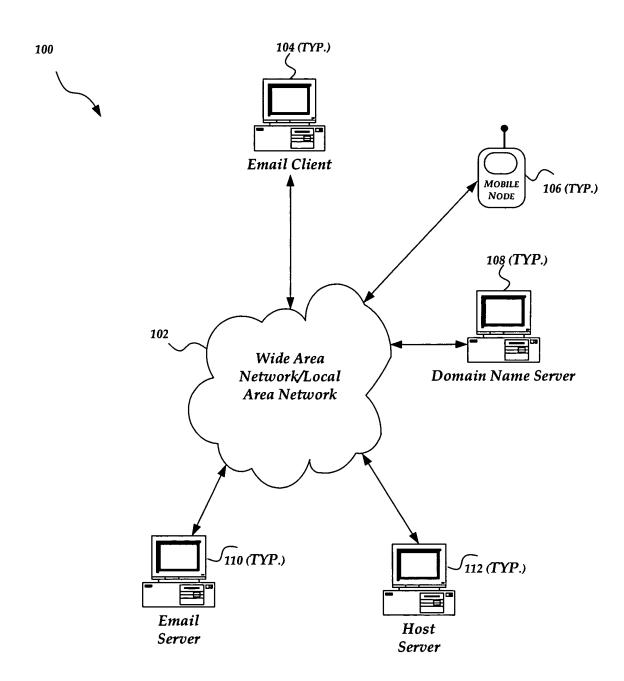
100

104 (TYP.)

Email Client

MOBILE NODE *106 (TYP.)*

108 (TYP.)

102

Wide Area Network/Local Area Network

Domain Name Server

110 (TYP.)

Email Server

112 (TYP.)

Host Server

FIG. 1

2/7

START

DIGITALLY SIGN
OUTBOUND MESSAGE   202

EMBED DIGITAL SIGNATURE
IN OUTBOUND MESSAGE   204

EMBED SELECTOR IN
OUTBOUND MESSAGE   206

COMBINE SELECTOR WITH
SENDER ADDRESS DOMAIN   208
FOR DNS LOOKUP

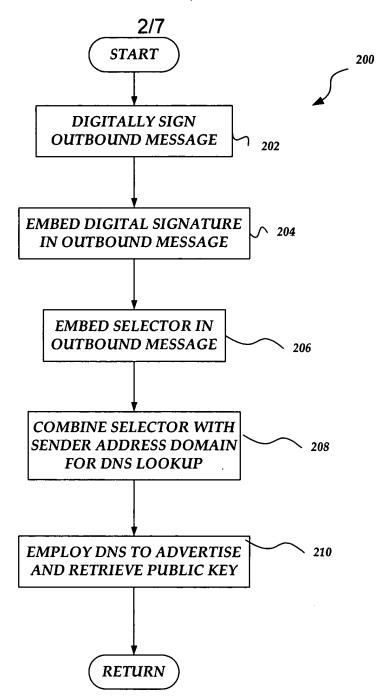EMPLOY DNS TO ADVERTISE   210
AND RETRIEVE PUBLIC KEY

RETURN

200

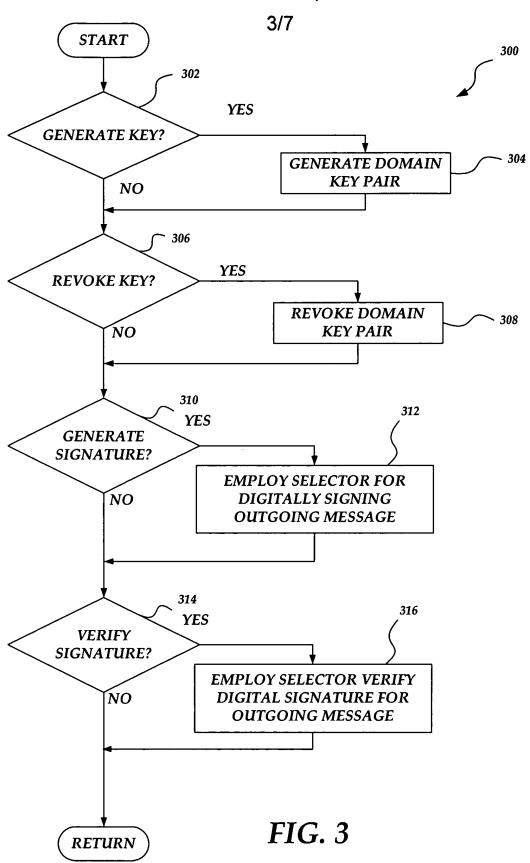*FIG. 2*

Title: SYSTEM AND METHOD FOR AUTHENTICATING THE DOMAIN OF A SENDER OF A MESSAGE
Inventors: Mark Delany
Docket No: D&D No. 08226/100S142-US1

3/7

START

302

GENERATE KEY?

YES

NO

300

GENERATE DOMAIN
KEY PAIR

304

306

REVOKE KEY?

YES

NO

REVOKE DOMAIN
KEY PAIR

308

310

GENERATE
SIGNATURE?

YES

NO

312

EMPLOY SELECTOR FOR
DIGITALLY SIGNING
OUTGOING MESSAGE

314

VERIFY
SIGNATURE?

YES

NO

316

EMPLOY SELECTOR VERIFY
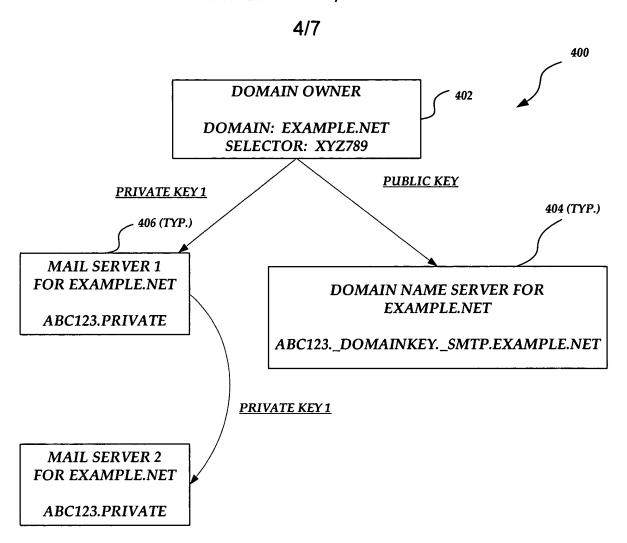DIGITAL SIGNATURE FOR
OUTGOING MESSAGE

RETURN

FIG. 3

Title: SYSTEM AND METHOD FOR AUTHENTICATING THE DOMAIN OF A SENDER OF A MESSAGE
Inventors: Mark Delany
D cket N : D&D No. 08226/100S142-US1

4/7

400

DOMAIN OWNER

DOMAIN: EXAMPLE.NET
SELECTOR: XYZ789

402

PRIVATE KEY 1

PUBLIC KEY

404 (TYP.)

406 (TYP.)

MAIL SERVER 1
FOR EXAMPLE.NET

ABC123.PRIVATE

DOMAIN NAME SERVER FOR
EXAMPLE.NET

ABC123._DOMAINKEY._SMTP.EXAMPLE.NET

PRIVATE KEY 1

MAIL SERVER 2
FOR EXAMPLE.NET

ABC123.PRIVATE

KEY GENERATION AND LOCATION OF
PUBLIC AND PRIVATE COMPONENTS

FIG. 4

DOMAIN OWNER

DOMAIN: EXAMPLE.NET
SELECTOR: XYZ789

502

500

PRIVATE KEY N-1

506 (TYP.)

PUBLIC KEY N-1
PUBLIC KEY N

504 (TYP.)

MAIL SERVER N-1
FOR EXAMPLE.NET

ABC123.PRIVATE

DOMAIN NAME SERVER FOR
EXAMPLE.NET

ABC123._DOMAINKEY._SMTP.EXAMPLE.NET

PRIVATE KEY N

MAIL SERVER N
FOR EXAMPLE.NET

ABC123.PRIVATE

KEY GENERATION AND LOCATION OF
PRIVATE COMPONENTS AT A
PARTICULAR MAIL SERVER

FIG. 5

Title: SYSTEM AND METHOD FOR AUTHENTICATING THE DOMAIN OF A SENDER OF A MESSAGE
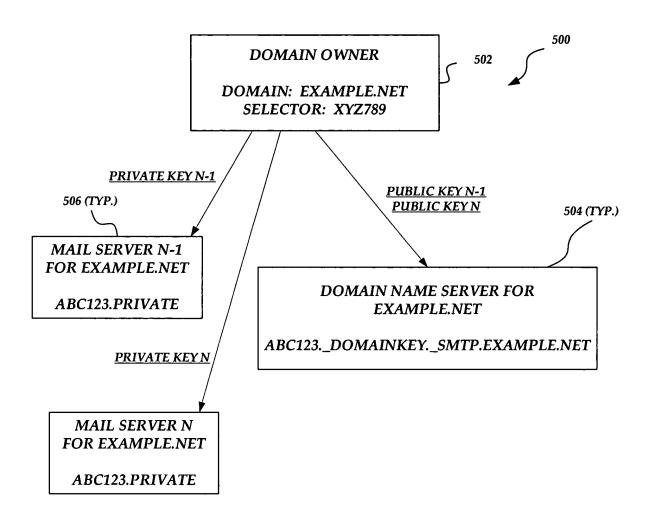Invent rs: Mark Delany
D cket No: D&D No. 08226/100S142-US1

6/7

FROM: JOE@EXAMPLE.NET
TO: BARRY@DISTANT.EXAMPLE.COM

SUBJECT: TEST EMAIL TO BARRY

602

606

600

MAIL SERVER N
FOR EXAMPLE.NET

ABC123.PRIVATE

604

HEADER
DOMAINKEY SIGNATURE:
SIGS-0.50:SYZ789:FEKC412DD....

FROM: JOE@EXAMPLE.NET
TO: BARRY@DISTANT.EXAMPLE.COM

SUBJECT: TEST EMAIL TO BARRY

608

MAIL SERVER
FOR
DISTANT.EXAMPLE.NET

610

TXT QUERY:
XYZ789.DOMAINKEY._SMTP.EXAMPLE.NET

612

DOMAIN NAME SERVER FOR
EXAMPLE.NET

ABC123._DOMAINKEY._SMTP.EXAMPLE.NET

AUTHENTICATION OF SENT MESSAGE

FIG. 6A

Title: SYSTEM AND METHOD FOR AUTHENTICATING THE DOMAIN OF A SENDER OF A MESSAGE
Inventors: Mark Delany
D cket No: D&D No. 08226/100S142-US1

7/7

600

608

MAIL SERVER FOR DISTANT.EXAMPLE.NET

614

HEADER

DOMAINKEY-STATUS: GOOD

DOMAINKEY SIGNATURE: SIGS-0.50:SYZ789:FEKC412DD....

FROM: JOE@EXAMPLE.NET
TO: BARRY@DISTANT.EXAMPLE.COM

SUBJECT: TEST EMAIL TO BARRY

616

RECIPIENT MAIL BOX

AUTHENTICATION OF SENT MESSAGE

FIG. 6B